# Solutions to MATH342 exam May 2012

| | |
|---|---|
| Bookwork<br>2marks<br><br>3marks | 1. $x \equiv y \mod n \quad \Leftrightarrow \quad n \mid (x-y)$.<br><br>$x_1x_2 - y_1y_2 = x_1(x_2 - y_2) + (x_1 - x_2)y_2$. So if $n \mid (x_1 - y_1)$ and $n \mid (x_2 - y_2)$ then $n \mid (x_1x_2 - y_1y_2)$. That is, if $x_1 \equiv x_2 \mod n$ and $y_1 \equiv y_2 \mod n$ then $x_1x_2 \equiv y_1y_2 \mod n$. |
| Standard homework exercises<br>2 marks<br>2 marks<br><br><br>2 marks<br><br>2 marks<br><br><br><br>7 marks | a) $x^2 \equiv 1 \mod 5 \quad \Leftrightarrow \quad (x-1)(x+1) \mod 5 \Leftrightarrow x = \pm 1 \mod 5$.<br><br>b) If $x = \pm 1 \mod 5$ or $x \equiv 0 \mod 5$ then $x^3 \equiv x \not\equiv 2 \mod 5$. If $x \equiv 2 \mod 5$, then $x^3 \equiv 3 \mod 5$. If $x \equiv 3 \mod 5$ then $x^3 \equiv 2 \mod 5$<br>c)$2x \equiv 3 \mod 4 \Leftrightarrow 2x = 3 + 4n$ for some $n \in \mathbb{Z}$. This has no solutions<br>d) $6x \equiv 8 \mod 14 \quad \Leftrightarrow \quad 3x \equiv 4 \mod 7 \quad \Leftrightarrow 5 \times 3x \equiv x \equiv 5 \times 4 \equiv 6 \mod 7$.<br>e)$2x \equiv 3 \mod 5 \quad \Leftrightarrow \quad 3 \times 2x \equiv x \equiv 3 \times 3 \equiv 4 \mod 5$. So<br>$x = 4 + 5y$ for some $y \in \mathbb{Z}$ and<br>$5(4 + 5y) \equiv 4 \mod 9 \Leftrightarrow -2y \equiv 2 \mod 9 \Leftrightarrow y = -1 + 9z$ for some $z \in \mathbb{Z}$. So this means that<br>$x = 4 + 5(-1 + 9z) = -1 + 45z$ for some $z \in \mathbb{Z}$ and<br>$3(-1 + 45z) \equiv 1 \mod 4 \Leftrightarrow 3(-1 + z) \equiv 1 \mod 4 \Leftrightarrow 3z \equiv 0 \mod 4 \Leftrightarrow x \equiv -1 \mod 180$. |

| | |
|---|---|
| Bookwork<br>4 marks<br><br>3 marks<br><br><br>1 mark | 2. FTA: Let $n \in \mathbb{Z}_+$ with $n \geq 2$. Then there are primes $q_i$ for $1 \leq i \leq m$ and $q_i < q_{i+1}$ and $k_i \in Z_+$ such that $n = \prod_{i=1}^m q_i^{k_i}$. This representation is unique.<br>Suppose that $p_{n+1} \geq \prod_{i=1}^n p_i = N$. Since $p_i$ divides $N$, it cannot divide $N+1$, and so $N+1$ is not divisible by $p_i$ for any $i \leq n$. So $p_{n+1} = N+1$. So in all cases, $p_{n+1} \leq N+1$.<br>$\pi(x)$ is the number of (positive) prime numbers $\leq x$, for any real number $x$. |
| Standard exercises<br>4 marks<br><br><br>2 marks | The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. So $\pi(23) = \pi(28) = 9$. Since $p_n$ is the $n$'th prime we have $\pi(p_n) = n$. If $n \geq 2$ then $p_n \geq 3$ is odd and $p_{n+1} \geq p_n + 2$. So if $n \geq 2$, $\pi(p_n + 1) = n$, but if $n = 1$, $\pi(p_1 + 1) = \pi(3) = 2$.<br>The first five primes in the sequence $p_n^{(3,4)}$ are 3, 7, 11, 19, 23. |
| Unseen<br><br><br>6 marks | Write $N = 4\prod_{i=2}^n p_i^{(3,4)} + 3$. Since 3 is not divisible by $p_i^{(3,4)}$ for any $i \geq 2$, $N$ is not divisible by $p_i^{(3,4)}$ for $i \geq 2$. Similarly, since the product is not divisible by 3, $N$ is not divisible by 3 either. Clearly, $N$ is odd. It cannot be the case that every prime which divides $N$ is equal to $1 \mod 4$ because the product of numbers which are 1 mod 4 is also $1 \mod 4$, and $N \equiv 3 \mod 4$. So there must be a prime which is $3 \mod 4$ which divides $N$ and is not $p_i^{(3,4)}$ for any $1 \leq i \leq n$. Therefore $p_{n+1}^{(3,4)}$ must exist. |

Bookwork: just the statement for $a \not\equiv 0$ will suffice
2 marks

3. Fermat's Little Theorem: Let $p$ be prime. Then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$, and $a^{p-1} \equiv 1 \mod p$ if $a \not\equiv 0 \mod p$.

---

Standard exercises
2 marks

(i) Since $a^{30} \equiv 1 \mod 31$ for $a \not\equiv 0 \mod 31$, we have $2^{60} \equiv 3^{150} \equiv 1 \mod 31$ we have $2^{62} + 3^{153} \equiv 2^2 + 3^3 \equiv 0 \mod 31$.

7 marks

(ii) The possible orders are all the divisors of 30, that is,

$$1,\ 2,\ 3,\ 5,\ 6,\ 10,\ 15,\ 30.$$

Of course 1 has order 1 and $-1$ has order 2. We see that $2^5 \equiv 1 \mod 31$, and hence 2 has order 5, and $-2$ has order 10. Since $3^3 \equiv -2^2$ and $-2^2$ also has order 10, we see that $3^3$ has order 10 and hence 3 has order 30. Then $3^2$ has order 15 and $3^5 = 243 \equiv -5$ has order 6, and $3^10 \equiv 25 \equiv -6$ has order 3. So elements of the respective orders are

$$1,\ -1,\ -6,\ 2,\ -5,\ -2,\ 9,\ 3.$$

5 marks

Clearly we cannot have $n \equiv 0 \bmod 7$. First suppose that $n \not\equiv 1 \bmod 7$. Then we need to find all $n \not\equiv 0$ and $m \geq 2$ such that $n^m \equiv 1 \bmod 7$. By Fermat's Little Theorem, $gcd(m, 6) = 2$, 3 or 6. If $m \equiv 0 \bmod 2$ then the only possibility for $n$ is $n \equiv -1 \equiv 6 \bmod 7$, since $-1 \bmod 7$ is the only element of order 2. If $m \equiv 0 \bmod 3$ then the two possibilities are $n \equiv 2$ and $n \equiv 4 \bmod 7$, since these are the elements of order 3. If $m \equiv 0 \bmod 6$ then the extra two possibilities (besides those already given) are $n \equiv 3 \bmod 7$ and $n \equiv 5 \bmod 7$. So altogether the possibilities for $(m, n)$ when $n \not\equiv 0 \bmod 7$ are

$$(0 \bmod 2, -1 \bmod 7),\ (0 \bmod 3, 2 \bmod 7),\ (0 \bmod 3, 4 \bmod 7),$$

$$(0 \bmod 6, 3 \bmod 7),\ (0 \bmod 6, 5 \bmod 7).$$

4 marks

Now let $n \equiv 1 \bmod 7$. Then for any $m \geq 1$

$$\frac{n^m - 1}{n - 1} = \sum_{i=0}^{m-1} n^i$$

and $n^i \equiv 1 \bmod 7$ for all $i$. So

$$\sum_{i=0}^{m-1} n^i \equiv m \bmod 7$$

and this is divisible by 7 if and only if $m \equiv 0 \bmod 7$.

Bookwork
1 mark

4. For any integer $n \in \mathbb{Z}_+$, $\phi(n)$ is the number of $k \in \mathbb{Z}_+$ with $k \leq n$ such that $gcd(k,n) = 1$

2 marks

If $p$ is prime and $a \geq 1$, then for $k \leq p^a$, we have

$$gcd(k,p^a) > 1 \Leftrightarrow p \mid k \ \Leftrightarrow k = \ell p, \quad 1 \leq \ell < p^{a-1}.$$

So

$$\phi(p^a) = p^a - 1 - (p^{a-1} - 1) = p^{a-1}(p-1).$$

2 marks

The divisors of $p^a$ are $p^i$ for $0 \leq i \leq a$, and

$$\int p^a = \sum_{i=0}^{a} p^i = \frac{p^{a+1}-1}{p-1}$$

3 marks

If

$$n = \prod_{i=1}^{m} p_i^{k_i}$$

where the $p_i$ are all distinct primes and $m_i \geq 1$ then

$$\phi(n) = \prod_{i=1}^{m} p_i^{k_i-1}(p_i - 1),$$

and

$$\int n = \prod \frac{p_i^{k_i+1}-1}{p_i - 1}.$$

Unseen except on practice exam
3 marks each

$9! = 2 \times 3 \times 2^2 \times 5 \times 2 \times 3 \times 7 \times 2^3 \times 3^2 = 2^7 \times 3^4 \times 5 \times 7$. So $\phi(9) = 2^6 \times 3^3 \times 2 \times 4 \times 6 = 2^10 \times 3^4 = 1024 \times 81 = 82944$. Then

$$\frac{9!}{3!6!}. = \frac{9 \times 8 \times 7}{6} = 12 \times 7 = 2^2 \times 3 \times 7$$

and

$$\phi\left(\binom{9}{3}\right) = \phi(2^2 \times 3 \times 7) = 2 \times 2 \times 6 = 24.$$

---

Unseen

In the expression above for $\phi(n)$ we have $p_i^{k_i-1}(p_i-1) \geq 2^{k_i}$ whenever $p_i > 2$ and $p_i^{k_i-1}(p_i-1) = 2^{k_i-1}$ if $p_i = 2$. So altogether this gives $2^{K-1} \leq \phi(n)$. Since $P-1$ is one of the factors in $\phi(n)$ we also

3 marks

have $\phi(n) \geq P-1$. We always have $\phi(n) \leq n$ since $\phi(n)$ is the number of elements in a certain subset of $\{k \in \mathbb{Z}_+ : k \leq n\}$. Since $p_i \leq P$ for all $i$, we also have $n \leq P^K$.

For any $K_0$, if $K \leq K_0$ and $n \geq K_0^{K_0}$ then $n^{1/K} \geq K_0$. So if $n$ is

3 marks

large enough given $K_0$, $\phi(n) > K_0$. Hence $\lim_{n\to\infty} \phi(n) = +\infty$.

| | |
|---|---|
| Bookwork<br>4 marks<br><br><br>2 marks | 5. If $x \equiv y \mod n_1$ and $x \equiv y \mod n_2$ then $n_1 \mid x-y$ and $n_2 \mid x-y$. Since $n_1$ and $n_2$ are coprime, this means that $n_1n_2 \mid x-y$ and hence $x \equiv y \mod (n_1n_2)$, and hence $F$ is injective. Since $\mathbb{Z}_{n_1n_2}$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ both have $n_1n_2$ elements, $F$ must be a bijection.<br>Since $F(1) = (1,1)$ and $F$ preserves multiplication, $F$ maps the group of units $G_n$ in $\mathbb{Z}_n$ to the group of units in $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, that is, to $G_{n_1} \times G_{n_2}$. |
| Standard exercise<br>4 marks | We have<br>$$F(0)=(0,0),\ F(1)=(1,1),\ F(2)=(2,2),\ F(3)=(0,3),\ F(4)=(1,4),$$ $$F(5)=(2,5),\ F(6)=(0,6),\ F(7)=(1,0),\ F(8)=(2,1),\ F(9)=(0,2),$$ $$F(10)=(1,3),\ F(11)=(2,4),\ F(12)=(0,5),\ F(13)=(1,6),$$ $$F(14)=(2,0),\ F(15)=(0,1),\ F(16)=(1,2),\ F(17)=(2,3),$$ $$F(18)=(0,4),\ F(19)=(1,5),\ F(20)=(2,6).$$ |
| Bookwork<br>2 marks | Korselt's condition on $n$ is that $n = \prod_{i=1}^{m} p_i$ where all the $p_i$ are distinct primes, and $p_i - 1 \mid n-1$ for all $i$. |
| Standard exercise<br>3 marks | $1729 = 7\times 247 = 7\times 13\times 19$, and $1728 = 8\times 216 = 2^6\times 27 = 2^6\times 3^3$. So 6 and $12 = 2^2 \times 3$ and $18 = 2 \times 3^2$ all divide 1728, and 1729 is a Carmichael number. |
| Unseen<br>1 marks | If $a^{n-1} = b^{n-1} \equiv 1 \mod n$ then $(ab^{-1})^{n-1} \equiv 1 \mod n$. So the set of pseudoprimes is a group |
| Standard exercise<br>4 marks | As above, we have $G_{21} \cong G_3 \times G_7$. Since 3 and 7 are prime, the groups $G_3$ and $G_7$ are cyclic of orders $2 = 3-1$ and $6 = 7-1$. So the order of any element of $G_{21}$ is a divisor of $lcm(6,2) = 6$. Now $21 = 20 = 2^2 \times 5$. For $a \in G_{21}$, 21 is a pseudoprime to base $a$ (pr $a \equiv 1$) if and only if $a^{20} \equiv 1 \mod 21$. Since $gcd(6,20) = 2$ this happens if and only if $a^2 \equiv 1 \mod 21$. Since $a^2 \equiv 1 \mod 3$ for both elements of $G_3$, and $a^2 \equiv 1 \mod 7$ for just two elements of $G_7$. So there are four such elements of $G_{21}$, and they are the elements mapped by $F$ to $(\pm 1, \pm 1)$. In fact since<br>$$G_{21} = \{\pm 1, \pm 2, \pm 4,\ \pm 5,\ \pm 8, \pm 10\}$$<br>we can also easily check that the elements are $\{\pm 1, \pm 8\}$. |

| | |
|---|---|
| Standard exercise<br>4 marks | 6.a) If $s = 2s_1$ is even then $s^2 = 4s_1^2 \equiv 0 \bmod 4$. If $s = 2s_1 + 1$ is odd then $$s^2 = 4s_1^2 + 4s_1 + 1 \equiv 1 \bmod 4.$$ Similar properties hold for $t$. So $s^2 + t^2$ is either $0 \bmod 4$ (of both $s$ and $t$ are even) or $2 \bmod 4$ (if both $s$ and $t$ are odd) or $1 \bmod 4$ if one of $s$ and $t$ is odd, and the other is even. |
| Bookwork<br>3 marks | b) Since conjugation is multiplicative, $$n = (s+it)(u+iv) \;\Leftrightarrow\; n = (s-it)(u-iv).$$ So $s+it$ divides $n$ if and only if $s-it$ does, and $$s+it \mid n \Rightarrow s^2+t^2 \mid n^2.$$ |
| 3 marks | If $$n_j = s_j^2 + t_j^2 = (s_j + it_j)\overline{s_j + it_j}$$ then $$n_1n_2 = (s_1+it_1)(s_2+it_2)\overline{(s_1+it_1)(s_2+it_2)} = (s_1s_2-t_1t_2)^2+(s_1t_2+s_2t_1)^2.$$ |
| Bookwork<br>3 marks | c) Since $s+it$ is prime in $\mathbb{Z}[i]$, we have $gcd(s,t) = 1$. If $$(s+it)(s-it)s^2+t^2 = uv$$ for integers $u$ and $v \geq 2$, then neither $u$ nor $v$ divides $s+it$ in $\mathbb{Z}[i]$, contradicting unique factorisation. So $s^2+t^2$ must be prime, and since $s^2+t^2 \mid n^2$ by b), we have $s^2+t^2 \mid n$. |
| Bookwork<br>5 marks<br><br>Standard exercise<br>2 marks | d) If $k^2 \equiv -1 \bmod p$ then there is $a \in \mathbb{Z}_+$ such that $k^2 + 1 = (k+i)(k-i) = ap$. Then $$k+i = \prod_j = 1^n(s_j + it_j),$$ where $s_j$ and $t_j \in \mathbb{Z} \setminus \{0\}$ for $1 \leq j \leq n$, and $s_j + it_j$ is prime in $\mathbb{Z}[i]$, and hence $$k - i = \prod_{j=1}^{n}(s_j - it_j).$$ So $$ap = \prod_{j=1}^{n}(s_j^2 + t_j^2).$$ By c) each $s_j^2 + t_j^2$ is prime in $\mathbb{Z}$. Hence $p = s_j^2 + t_j^2$ for some $j$.<br>We have $21 \equiv 1 \bmod 4$ but $21 = 3 \times 7$ and $3 \equiv 7 \bmod 4$. |

| | |
|---|---|
| standard theory<br>Bookwork<br>2 marks | 7. The Legendre symbol is defined by<br>$\left(\frac{q}{p}\right) = \begin{matrix} 1 & \text{if } q \equiv a^2 \mod p \text{ for some } a \in \mathbb{Z} \\ -1 \text{ otherwise} & \end{matrix}$ |
| Bookwork<br>5 marks | If $q \equiv a^2 \mod p$ then $q^{(p-1)/2} \equiv a^{p-1} \equiv 1$ by Fermat's Little Theorem. Conversely if $q^{(p-1)/2} \equiv 1$ and $b$ is a primitive element of $G_p$ and $q = b^m$ then $b^{m(p-1)/2} \equiv 1$ implies that $p-1 \mid m(p-1)/2$, that is, $m$ must be even and hence $q \equiv (b^{(m-1)/2})^2$. Since<br>$F(q_1 q_2) \equiv (q_1 q_2)^{(p-1)/2} \equiv q_1^{(p-1)/2} q_2^{(p-1)/2} \equiv F(q_1)F(q_2) \bmod p$<br>we see that $q \mapsto F(q) \bmod p$ is a homomorphism. Since $-1 \not\equiv 1 \bmod p$ we see that $F$ itself is a homomorphism. |
| Bookwork<br>3 marks | For any odd prime $p$,<br>$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p = \pm 1 \mod 8.$<br>If $p$ and $q$ are odd primes, then<br>$\left(\frac{q}{p}\right) \times \left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$ |
| Standard exercise 3 marks | $\left(\frac{6}{17}\right) = \left(\frac{2}{17}\right) \times \left(\frac{3}{17}\right)$<br>and since $17 \equiv 1 \bmod 8$ we have<br>$\left(\frac{2}{17}\right) = 1 \text{ and } \left(\frac{3}{17}\right) \times \left(\frac{17}{3}\right) = (-1)^{8\times 1} = 1,$<br>and since $17 \equiv 2 \bmod 3$ and $3 \equiv 3 \bmod 8$, we have<br>$\left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1 \text{ and } \left(\frac{6}{17}\right) = -1.$ |

| | |
|---|---|
| Standard exercise<br>3 marks | Since both 23 and 73 are prime we have $$\left(\frac{23}{73}\right) \times \left(\frac{73}{23}\right) = (-1)^{11\times 36} = 1.$$ Then since $73 = 3\times 23 + 4$ and $23 \equiv -1 \bmod 8$ $$\left(\frac{73}{23}\right) = \left(\frac{4}{23}\right) = \left(\frac{2}{23}\right)^2 = 1^2 = 1 \text{ and } \left(\frac{73}{23}\right) = 1.$$ |
| Will be exercise near end of course<br>4 marks | $$\left(\frac{-3}{p}\right) \times \left(\frac{p}{-3}\right) = (-1)^{(-3-1)/2\times(p-1)/2} = 1$$ and $$\left(\frac{p}{-3}\right) = \left(\frac{p}{3}\right) = \begin{matrix} 1 \text{ if } p \equiv 1 \mod 3 \\ -1 \text{ if } p \equiv 2 \bmod 3 \end{matrix}.$$ Now suppose that there are finitely many such primes $q_i$, with $1 \leq i \leq n$ and let $p$ be any prime dividing $N^2+3$, where $$N = \prod_{i=1}^{n} q_i.$$ Then $p \mid N^2+3$ is equivalent to $N^2 \equiv -3 \mod p$ and hence $p \equiv 1$ mod 3. But then $p \mid N$, which is a contradiction since $p \not| 3$. |